



**NÁRODNÝ BEZPEČNOSTNÝ ÚRAD
SLOVENSKEJ REPUBLIKY**

SEP 1.3.2.9

VZOR PROTOKOLU O KOMPILÁCII

3. novembra 2005

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Sekcia informačnej bezpečnosti a elektronického podpisu

Budatínska č. 30, 850 07 Bratislava 57

<http://www.nbusr.sk/sep/default.html>

e-mail: sep@nbusr.sk

Obsah

1	Predmet dokumentu	4
2	Skratky.....	5
3	Vzor protokolu o kompilácii	6
Príloha A	Literatúra	11
Príloha B	História	12

1 Predmet dokumentu

Účelom tohto dokumentu je zaviesť jednotný postup pri kompilácii zdrojových kódov SW aplikácií určených na vyhotovovanie a/alebo overovanie zaručeného elektronického podpisu v súlade so zákonom [1]. Výsledkom procesu kompilácie je skompilovaný zdrojový kód. Z procesu kompilácie musí byť vyhotovený protokol o kompilácii, ktorého vzor je súčasťou tohto dokumentu.

2 Skratky

DVD/CD	elektronické nosiče dát
HW	hardvér
SW	softvér
HDD	pevný disk počítača
PC	osobný počítač

3 VZOR PROTOKOLU O KOMPILÁCI

(Záhlavie: organizácia, ktorá vyhotovila protokol o kompilácii)

Počet listov: x
Počet príloh: x

PROTOKOL O KOMPILÁCI

Predmet kompilácie: *(uviesť presný názov a verziu produktu)*

Účel produktu kompilácie: *(uviesť stručnú charakteristiku produktu)*

Výrobca: *(uviesť obchodný názov a adresu výrobcu produktu)*

Audítor: *(uviesť obchodný názov a adresu audítora)*

Miesto kompilácie: *(uviesť miesto vykonania kompilácie)*

Dátum a čas kompilácie: *(uviesť dátum a čas vykonania kompilácie)*

Prítomní: *(uviesť zoznam prítomných osôb zúčastnených pri procese kompilácie)*

(Zápätie: Nastaviť číslo stránky/počet strán)

Zoznam nástrojov potrebných na kompiláciu:

č.	Názov	Verzia	Stručný popis	Poznámka
1	Napr.: MS Windows	XP + SP2	Operačný systém	Štandardný komerčný produkt
2	Napr.: xy.dll	1.0.20	Plugin pre XY.	Interný nástroj
3				
4				
5				
6				
7				

Poznámka k interným nástrojom:

(Ak sú v zozname uvedené interné nástroje výrobcu je potrebné uviesť do poznámky ich stručnú charakteristiku.)

Konkrétne nástroje potrebné na kompiláciu a zdrojové kódy interných nástrojov výrobcu sú uložené v elektronickej forme na DVD/CD. (**Príloha č. 1**)

Zoznam ďalších pomocných nástrojov:

č.	Názov	Verzia	Stručný popis	Poznámka
1	Napr.: Nero Burning Rom	5.0	Nástroj na zálohovanie dát na CD/DVD nosič	Štandardný komerčný produkt
2				
3				

Konkrétne pomocné nástroje sú uložené v elektronickej forme na DVD/CD. (**Príloha č. 2**)

Postup kompilácie:

1. Príprava prostredia a HW prostriedkov.
2. Formátovanie HDD príslušného PC (HW).
3. Inštalácia požadovaného SW vybavenia:
 - a) ...
 - b) ...
 - c) ...

Poznámka: Počas inštalácie môžu byť priebežne vytvárané image súbory HDD, ktoré budú zálohované na DVD/CD nosičoch dát. (Príloha č. 3/x). (Kde „x“ je poradové číslo DVD/CD nosiča s priebežnou zálohou.)

4. Príprava zdrojových kódov. Nakopírovanie obsahu DVD/CD so zdrojovými kódmi do adresára (uviesť lokalizáciu adresára). (Príloha č. 4)
5. Audítora alebo zástupca NBÚ vykoná kontrolu integrity a úplnosti skopírovaných zdrojových kódov. Nástrojom audítora alebo NBÚ sa porovnajú zdrojové kódy posudzované v procese auditu s nahranými zdrojovými kódmi.
6. Vytvorenie kľúča na podpis komponentov aplikácie a/alebo celej aplikácie (aktuálne napr. v prostredí .NET).
7. Vytvorenie samotného verejného kľúča z vygenerovaného kľúčového páru (aktuálne napr. v prostredí .NET).
8. Audítora alebo zástupca NBÚ vytvorí zálohu kľúčového páru na externý nosič dát. (Príloha č. 8) (aktuálne napr. v prostredí .NET)
9. Spustenie kompilácie projektu a vytvorenie inštalačného programu.
10. Vytvorenie DVD/CD so skompilovanými kódmi. (Príloha č. 5)
11. Vytvorenie inštalačného DVD/CD aplikácie. (Pokiaľ to dovoľuje charakter aplikácie.) (Príloha č. 6)
Poznámka: Postup môže byť rozširovaný podľa potreby a vlastností kompilačného prostredia.
12. Otestovanie inštalačného DVD/CD aplikácie.
13. Vytvorenie hash (SHA 1) odtlačkov skompilovaných a inštalačných súborov.
14. Vytvorenie alebo skopírovanie minimálne 3 kusov inštalačného DVD/CD aplikácie.
15. Audítora alebo zástupca NBÚ zabezpečí bezpečné zmazanie kľúčového páru z HDD (aktuálne napr. v prostredí .NET).
16. Formátovanie HDD príslušného PC.

Zdrojové kódy a súbory vstupujúce do procesu kompilácie a vytvorenia inštalačného balíka:

Zdrojové kódy a súbory potrebné na skompilovanie aplikácie (uviesť názov a verziu produktu) a vytvorenie inštalačného balíka príslušnej aplikácie sú uložené v elektronickej forme na DVD/CD nosiči. (Príloha č. 4). Hash odtlačky všetkých súborov sú uvedené v prílohe č. 7.

Zoznam výsledných skompilovaných súborov a ich hash otláčkov:**a) trusted:**

Č.	Názov súboru	Hash (Sha1)
1		
2		
3		
4		
5		

b) non-trusted:

Č.	Názov súboru	Hash (Sha1)
1		
2		
3		
4		
5		
6		
7		
8		

Zoznam skompilovaných inštalačných súborov a ich hash otláčkov:

Č.	Názov súboru	Hash (Sha1)
1	<i>Napr.: Setup.exe</i>	

Poznámka: V závislosti od charakteru produktu nemusí byť vždy vytvorený/skompilovaný inštalačný súbor napríklad pri aplikáciách využívajúcich prostredie Java.

Zoznam príloh:

1. **Príloha č. 1** – DVD/CD - nástroje potrebné na kompiláciu
2. **Príloha č. 2** – DVD/CD - pomocné nástroje
3. **Príloha č. 3/x** – DVD/CD - image súbory HDD
4. **Príloha č. 4** – DVD/CD - zdrojové kódy aplikácie
5. **Príloha č. 5** – DVD/CD - skompilované zdrojové kódy aplikácie
6. **Príloha č. 6** – DVD/CD - inštalačné CD aplikácie
7. **Príloha č. 7** – zoznam zdrojových kódov a ich hash otláčkov
8. **Príloha č. 8** – externý nosič dát - záloha kľúčového páru (*aktuálne napr. v prostredí .NET*)

Po skončení kompilácie boli uvedené prílohy zapečatené a podpísané výrobcom a boli odovzdané k uloženiu *audítovi/NBÚ*. Môžu byť otvorené len pre účely preukazovania dôveryhodnosti a pravosti skompilovaných súborov a ich hash otláčkov, za prítomnosti *oprávnenej osoby zastupujúcej výrobcu a organizáciu v ktorej sú prílohy uložené*.

Záver:

Všetci prítomní konštatovali, že proces kompilácie prebehol v súlade s protokolom o kompilácii a výsledkom kompilácie je v protokole uvedený skompilovaný zdrojový kód a inštalačný súbor aplikácie (*uviesť názov a verziu produktu*), určenej pre proces certifikácie produktu pre zaručený elektronický podpis a svojím podpisom uvedené potvrdzujú.

V (*uviesť miesto*) dňa (*uviesť dátum*).

podpis zástupcu výrobcu

podpis zástupcu audítora

podpis zástupcu NBÚ

Poznámka: *Prítomnosť zástupcu audítora pri procese kompilácie je nutná podmienka. Prítomnosť NBÚ nie je vyžadovaná.*

Príloha A Literatúra

- [1] Zákon č. 215/2002 o elektronickom podpise a o zmene a doplnení niektorých zákonov

Príloha B História

Verzia:	Dátum vydania:	Poznámka:	Vypracoval:
SEP 1.3.2.9	3.11.2005	Prvé vydanie	Ing. Anton Lachký, Mgr. Ivan Chrenko